CORE
Metadata, citation and similar papers at core.ac.uk
Provided by eJournals System Universitas Mulawarman

Sains, Aplikasi, Komputasi dan Teknologi Informasi
Vol 2, No 2, April 2020, pp. 52-56
ISSN: 2684-8473

Metode steganografi citra digital

Anita Putri Ratnasari[a1], Felix Andika Dwiyanto[b2]

[a] *Jurusan Teknik Elektro, Universitas Negeri Malang, Indonesia*
[b] *Pendidikan Kejuruan, Universitas Negeri Malang, Indonesia*
[1] *anitaapr72@gmail.com;* [2] *ayikgugun@gmail.com*

INFORMASI ARTIKEL

Histori Artikel
Diterima : 22 Februari 2020
Direvisi : 29 Februari 2020
Diterbitkan : 4 April 2020

Kata Kunci:
Steganografi
Citra Digital
LSB
MSB
DCT
DWT
Spread Spectrum
BPCS

ABSTRAK

Steganografi merupakan teknik penyembunyian data dalam media. Dalam penyembunyiannya, pesan rahasia disisipkan pada media pembawa (carrier file) antara lain, teks, gambar, audio dan video. Salah satu carrier file dalam steganografi adalah gambar/citra digital, yang merupakan media yang paling sering digunakan dalam pertukaran data melalui internet. Dalam review literatur ini, akan dijelaskan tentang metode steganografi pada citra digital, seperti LSB, MSB, DCT, DWT, Spread Spectrum dan BPCS. Termasuk penjelasan tentang perbandingan berupa kelebihan dan kelemahan dari masing-masing metode. Dengan melihat dan mempelajari beberapa metode tersebut diharapkan pengembangan yang dilakukan akan lebih baik dan dapat menutupi kekurangan sebelumnya.

2019 SAKTI – Sains, Aplikasi, Komputasi dan Teknologi Informasi.
Hak Cipta.

I. Pendahuluan

Untuk berbagai alasan, keamanan dan kerahasiaan sangat dibutuhkan dalam komunikasi data melalui internet, tak terkecuali sebuah pesan. Steganografi sebagai suatu seni penyembunyian pesan ke dalam suatu media yang banyak dimanfaatkan untuk mengirim pesan melalui jaringan internet tanpa diketahui orang lain [1], [2]. Menyembunyikan sebuah pesan dengan steganografi akan mengurangi kecurigaan dan peluang terdeteksinya keberadaan pesan oleh pihak ketiga [3]. Media yang digunakan sebagai media pembawa (*carrier file*) dapat berupa teks, gambar, audio dan video. Salah satu *carrier file* dalam steganografi adalah gambar/citra digital, merupakan media yang paling sering digunakan karena sering dipertukarkan dalam dunia internet antara lain, JPEG, PNG, GIF dan BMP.

Terdapat teknik dasar dalam steganografi, yaitu teknik substitusi, teknik *transform* domain, teknik *statistic*, teknik *distortion*, dan teknik *cover generation* [4]. Masing-masing teknik dasar diwakili metode, misal teknik substitusi menggunakan metode LSB dan MSB, teknik *transform* domain menggunakan metode *Spread Spectrum*, dll. Metode LSB, merupakan metode yang paling sering digunakan karena termasuk metode dasar dalam pengembangan metode-metode yang lainnya. Metode ini menggunakan bit paling tidak berarti untuk digantikan bit pesan yang akan disisipi. Sama-sama mengganti bit, metode MSB dikembangkan dari metode dasar tersebut. Namun, metode MSB menggunakan bit yang paling berarti untuk digantikan dengan bit pesan.

Tidak seperti LSB, metode *Spread Spectrum* akan mengacak pesan yang tersimpan dalam citra. Sehingga memiliki keamanan yang baik karena pesan sulit terdeteksi [5], namun memerlukan kunci untuk mendeskripsikan citra agar dapat membaca suatu pesan. Pada metode DCT dan DWT, akan menyisipkan pesan ke dalam sinyal dalam ranah *transform*. Dan untuk metode BPCS, penyisipan dilakukan tidak hanya pada *least significant bit*, tapi pada seluruh *bitplane* yang termasuk *noise-like regions*. Pada *review* literatur ini, akan dijelaskan tentang metode steganografi LSB, MSB, DCT, DWT, *Spread Spectrum* dan BPCS yang masing-masing akan dibandingkan kelebihan dan kelemahannya. Sehingga, dapat digunakan sebagai rujukan untuk penelitian mendatang.

II. Kajian Pustaka

Metode steganografi dapat digunakan pada citra digital. Metode steganografi pada citra digital terdiri dari metode sebagai berikut:

A. Least Significant Bit (LSB)

Pendekatan paling sederhana untuk menyembunyikan data dalam *file* citra disebut penyisipan *Least Significant Bit* (LSB)[6]. Metode ini banyak digunakan karena komputasinya tidak terlalu kompleks dan pesan

yang disembunyikan cukup aman [7]. Penyisipan *Least significant bit* (LSB) adalah pendekatan yang umum untuk menanamkan informasi dalam media citra. *Least significant bit* (dengan kata lain, bit ke-8) sebagian atau seluruh dari *byte* dalam sebuah gambar diubah menjadi sebuah *bit* dari pesan rahasia.

Untuk *file* bitmap 24 bit maka setiap *pixel* (titik) pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit *(byte)* dari 0 sampai 255 atau dengan format *biner* 00000000 sampai 11111111. Dengan demikian pada setiap *pixel file* bitmap 24 bit, dapat disisipi 3 bit data[10]. Sebagai ilustrasi misalkan *cover-object* adalah sekempulan citra seperti yang terlihat pada contoh berikut:

00110011 10100010 11100010 01101111

Misalnya pesan rahasia (yang telah dikonversi ke *system biner*) adalah 0110. Setiap bit dari *watermark* menggantikan posisi LSB dari segmen *pixel-pixel* citra menjadi:

00110010 10100011 11100011 01101110

Dari hasil diatas menunjukkan, bahwa bit terakhir sebagai bit yang tidak penting akan digantikan dengan *pixel* dari pesan rahasia [8].

B. Most Significant Bit (MSB)

Pada metode MSB, pesan disisipkan pada *bit* ke-1. Sebagai contoh, misalkan tiga piksel yang berdekatan (sembilan *bytes*) dengan kode RGB seperti pada metode LSB+1 akan disisipkan adalah karakter "R" dengan menggunakan metode MSB, maka akan dihasilkan citra hasil dengan urutan *bit* sebagai berikut:

00110101 **1**1010110 **0**1101010

11110100 **0**0111001 **0**1100001

11110001 **0**0010001 11100001

Pada contoh di atas, dapat dilihat bahwa sebagian MSB+1 (*bit* ke-1) yang ada pada citra asal *(original)* digantikan dengan bit dari pesan yang akan disisipkan [6].

C. Spread Spectrum

Metode *Spread Spectrum* adalah sebuah teknik pentransmisian dengan menggunakan *pseudonoise code,* yang independen terhadap data informasi, sebagai modulator bentuk gelombang untuk menyebarkan *energy* sinyal dalam sebuah jalur komunikasi (*bandwidth*) yang lebih besar daripada sinyal jalur komunikasi informasi [9]. Oleh penerima, sinyal dikumpulkan kembali menggunakan *replica pseudonoise code* tersinkronisasi. Metode *Spread Spectrum* memperlakukan *coverimage* baik sebagai derau *(noise)* ataupun sebagai usaha untuk menambahkan derau semu *(pseudonoise)* ke dalam *cover-image.*

Proses penyisipan pesan menggunakan metode *Spread Spectrum* ini terdiri dari tiga proses, yaitu *spreading*, modulasi, dan penyisipan pesan ke citra. Sedangkan proses ekstraksi pesan menggunakan metode *Spread Spectrum* ini terdiri dari tiga proses, yaitu pengambilan pesan dari matriks frekuensi, demodulasi, dan *de-spreading.*

D. Discrete Cosine Transform (DCT)

DCT merupakan sebuah metode yang telah diterapkan di berbagai bidang pengetahuan. DCT merupakan metode yang mentransfrormasikan sebuah informasi dari domain ruang atau waktu ke dalam domain frekuensi dengan tujuan untuk mempercepat transmisi, mengurangi penyimpanan di dalam memori, menyediakan representasi *compact*, dan sebagainya [10]. Metode DCT yang banyak digunakan dalam aplikasi adalah DCT 2D [4]. Persamaan untuk transformasi DCT 2D (citra berukuran m x n) ditunjukkan pada persamaan di bawah ini:

$$C(u,v) = \propto (u) \propto (v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \cos \frac{\pi(2x+1)u}{2N} \cos \frac{\pi(2y+1)}{2N} \quad (1)$$

dimana $\propto (u) = \sqrt{\frac{1}{N}}$ untuk u = 0, sedangkan $\propto (u) = \sqrt{\frac{2}{N}}$ untuk u = 1,2,3,...n-1

Untuk invers dari transformasi 2D DCT dapat dilihat pada persamaan di bawah ini:

$$C(u,v) = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} \propto (u) \propto (v) C(u,v) \cos \frac{\pi(2x+1)u}{2N} \cos \frac{\pi(2y+1)}{2N} \quad (2)$$

E. Discrete Wavelet Transform (DWT)

DWT merupakan metode yang dapat membagi informasi dari suatu citra menjadi pendekatan dan detail sinyal. *LL band* meliputi koefisien *low pass* dan pendekatan terhadap suatu citra serta detail sub *signal* lainnya yang menunjukkan rincian vertikal, horisontal, atau diagonal atau perubahan di dalam suatu citra [4]. Persamaan umum untuk DWT dapat dilihat pada persamaan di bawah ini:

$$DWT\{f(t)\} = W_{\emptyset}(j_{\emptyset}, k) + W_{\emptyset}(j, k) \quad (3)$$

F. Bit-Plane Complexity Segmentation (BPCS)

Teknik BPCS ini adalah teknik steganografi yang tidak berdasarkan teknik pemrograman, tetapi teknik yang menggunakan sifat penglihatan manusia [11]. Proses penyisipan pesan dilakukan pada segmen yang memiliki kompleksitas yang tinggi. Segmen yang memiliki kompleksitas tinggi ini disebut *noise-like regions*. Pada segmen-segmen ini penyisipan dilakukan tidak hanya pada *least significant bit*, tapi pada seluruh *bitplane* yang termasuk *noise-like regions*. Oleh sebab itu, pada teknik BPCS, kapasitas data yang disisipkan dapat mencapai 50% dari ukuran *cover-object*-nya [12]. Langkah-langkah yang dilakukan pada algoritma BPCS pada saat menyisipkan data adalah sebagai berikut:

- *Cover-object* dengan sistem PBC diubah menjadi sistem CGC, kemudian citra tersebut di-*slice* menjadi *bit-plane* dalam bentuk citra *biner*. Setiap *bit-plane* mewakili bit dari setiap piksel pada citra.
- Segmentasi setiap *bit-plane* pada *cover-object* menjadi *informative* dan *noise-like region* dengan menggunakan nilai batas/*threshold* ($\alpha 0$). Nilai umum dari *threshold* =0,3.
- Kelompokkan *byte-byte* pesan rahasia menjadi rangkaian blok pesan rahasia.
- Jika blok (S) kurang kompleks dibandingkan dengan nilai batas, maka lakukan konjugasi terhadap S untuk mendapatkan S* yang lebih kompleks. Blok konjugasi (S*) pasti lebih kompleks dibandingkan dengan nilai batas.
- Sisipkan setiap blok pesan rahasia ke *bit-plane* yang merupakan *noise-like region* (atau gantikan semua bit pada *noise-like region*). Jika blok S dikonjugasi, maka simpan data pada *conjugation map*.
- Sisipkan juga *conjugation map* seperti yang dilakukan pada blok pesan rahasia.
- Ubah *stego-object* dari sistem CGC menjadi sistem PBC.

Selanjutnya dapat dilakukan proses ekstraksi pesan rahasia. Proses ekstraksi pesan rahasia dapat dilakukan dengan menerapkan langkah-langkah penyisipan secara terbalik.

III. Analisis Perbandingan

Selanjutnya, akan diberikan kelebihan dan kelemahan dari masing-masing metode. Selengkapnya dapat dilihat pada Tabel 1. Berdasarkan Tabel 1 dapat dilihat beberapa metode yang dibandingkan adalah (a) Least Significant Bit (LSB), (b) Most Significant Bit (MSB), (c) Spread Spectrum, (d) Discrete Cosine Transform (DCT), (e) Discrete Wavelet Transform (DWT), dan (f) Bit-Plane Complexity Segmentation (BPCS).

Tabel 1 Perbandingan Metode-Metode

Metode	Kelebihan	Kelemahan
Least Significant Bit (LSB)	• Memiliki nilai MSE kecil dan PSNR besar, sehingga kualitas citra sebelum penyisipan pesan tidak jauh berbeda dengan citra sesudah penyisipan pesan [1], [13]–[16] • Proses penyisipan dan ektraksi cepat [4] • Citra sebelum dan sesudah penyisipan pesan memiliki resolusi yang sama [17], [18] • Cepat dan mudah [19], [20] • Ukuran citra asli dan citra berisi pesan sama [7], [21] • Tidak hanya terpaku pada 1 bit terakhir saja sebagai tempat penyembunyian data, namun bisa dikembangkan hingga 8 bit [22]	• Tingkat ketahanan pesan terhadap perubahan kontras citra buruk, sehingga kerusakan pesan besar dan tidak dapat dibaca [6] • Mudah diserang dalam pemrosesan image, seperti cropping dan kompresi [4], [16], [19], [23] • Analisis keamanan kurang baik dengan pendeteksian perhitungan PSNR [7], [20] • Kapasitas pesan yang disisipkan terbatas [21]
Most Significant Bit (MSB)	• Tingkat ketahanan pesan terhadap perubahan kontras citra baik, sehingga kerusakan pesan kecil dan masih dapat dibaca [6]	• Memiliki nilai MSE besar, sehingga kualitas citra sebelum penyisipan pesan jauh berbeda dengan citra sesudah penyisipan pesan [1], [14]
Spread Spectrum	• Nilai PSNR tinggi dan MSE kecil, sehingga citra hasil steganografi mampu menyerupai citra aslinya [5], [9] • Performasi robustness pada citra baik karena hanya memiliki perubahan pixel sangat kecil [9] • Peluang terdeteksinya pesan rendah [24]	• Tidak memiliki performansi yang baik ketika diberikan serangan berupa *noise*, *cropping* dan proses kompresi [9], [20] • Memiliki proses *embedding* dan ekstraksi yang lama [20]

Metode	Kelebihan	Kelemahan
Discrete Cosine Transform (DCT)	• Butuh waktu singkat untuk pemrosesan [4] • Memiliki keamanan yang baik [16]	• Memiliki nilai PSNR kecil sehingga citra hasil steganografi kurang menyerupai citra aslinya [4]
Discrete Wavelet Transform (DWT)	• Memiliki nilai PSNR besar sehingga citra hasil steganografi mampu menyerupai citra aslinya [4], [25] • Memiliki keamanan yang baik [25] • Cocok untuk menyisipkan kapasitas pesan yang besar [26]	• Butuh waktu lama dalam pemrosesan [4] • Jumlah karakter pesan mempengaruhi kualitas citra [27]
Bit-Plane Complexity Segmentation (BPCS)	• Memiliki waktu ekstraksi yang cepat [11] • Cocok untuk menyisipkan kapasitas pesan yang besar [26]	• Waktu penyisipan pesan yang lambat [11] • Berubahnya ukuran file citra setelah disisipi pesan [11]

IV. Kesimpulan

Steganografi merupakan ilmu dan bisa dikatakan seni menyembunyikan pesan rahasia dengan suatu cara sedemikian sehingga tidak seorang pun yang mencurigai keberadaan pesan tersebut. Media untuk menyisipkan pesan dapat berupa teks, citra digital, audio maupun video. Dalam *paper review* ini, menggunakan studi *literature* tentang steganografi pada citra digital. Berdasarkan *paper review* ini dapat diketahui bahwa terdapat banyak metode steganografi pada citra digital, namun dalam *review* literatur ini telah dibahas 6 metode antara lain LSB, MSB, *Spread Spectrum*, DCT, DWT dan BPCS. Masing-masing metode mempunyai kelebihan dan kekurangan, sehingga tidak ada metode yang sempurna dan penggunaannya tergantung kebutuhan.

Daftar Pustaka

[1] K. Anand, Ér, and R. Sharma, "Comparison of LSB and MSB Based Image Steganography," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 4, no. 8, 2014.

[2] N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Steganography," *IEEE Secur. Priv.*, vol. 1, no. 3, pp. 32–44, 2003.

[3] C. Cachin, "Digital Steganography," *Encycl. Cryptogr. Secur.*, pp. 159–164, 2005.

[4] P. Batarius and M. Maslim, "Perbandingan Metode dalam Teknik Steganografi," in *Seminar Nasional Teknologi Informasi & Komunikasi Terapan 2012 (Semantik 2012)*, 2012, pp. 307–313.

[5] T. Morkel, J. Eloff, and M. Olivier, "An Overview of Image Steganography," in *Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005)*, 2005, pp. 1–12.

[6] Y. Andrian and S. Fadly, "Analisis Ketahanan Citra Stego Metode LSB, LSB+1, LSB+2 dan MSB Terhadap Perubahan Kontras Citra," 2009.

[7] H. Antonio, "Studi Perbandingan Enkripsi Steganografi dengan menggunakan Metode Least Significant Bit dan End of File."

[8] P. Alatas, "Implementasi Teknik Steganografi dengan Metode LSB pada Citra Digital," Universitas Gunadarma, 2009.

[9] A. Septayuda, B. Hidayat, and H. H. Nuha, "Analisis Steganografi Citra Digital menggunakan Metode Spread Spectrum berbasis Android," in *e-Proceeding of Engineering*, 2014, pp. 1–16.

[10] R. Uma, "FPGA Implementation of 2-D DCT for JPEG Image Compression," *Int. J. Adv. Eng. Sci. Technol.*, vol. 7, no. 1, pp. 1–9, 2011.

[11] S. Dewi, A. U. A. Wibowo, and H. Rachmawati, "Analisis Perbandingan Steganografi Pada Citra Digital Gif dan Tiff Dengan Metode BPCS," *J. Aksara Komput. Terap.*, vol. 1, no. 2, 2012.

[12] E. Kawaguchi and R. O. Eason, *Principle and applications of BPCS Steganography*. Kitakyushu: Kyushu Institute of Technology, 1998.

[13] E. Y. Hidayat and K. Hastuti, "Analisis Steganografi Metode Least Significant BIT (LSB) dengan Penyisipan Sekuensial dan Acak secara Kuantitatif dan Visual," *Techno.COM*, vol. 12, no. 3, pp. 157–167, 2013.

[14] A. Khurana and B. M. Mehta, "Comparison of LSB and MSB based Image Steganography," *IJCST*, vol. 3, no. 3, pp. 870–871, 2012.

[15] D. Rawat and V. Bhandari, "A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image," *Int. J. Comput. Appl.*, vol. 64, no. 20, 2013.

[16] G. Kaur and A. Kochhar, "A Steganography Implementation based on LSB & DCT," *Int. J. Sci. Emerg. Technol. with Latest Trends*, vol. 4, no. 1, pp. 35–41, 2012.

[17] R. Zulfachrein, "Implementasi Algoritma Least Significant Bit (LSB) dalam Pembuatan Aplikasi Steganografi berbasis Android," 2015.

[18] D. K. Basuki and I. U. Nadhori, "Data Hiding Steganograph pada File Image menggunakan Metode Least Significant Bit," Institut Teknologi Sepuluh Nopember, 2009.

[19] R. S. Basuki and E. N. Maranggani, "Embedding Pesan Rahasia di dalam suatu Gambar dengan Metode Least Significant Bit Insertion (LSB)," in *Seminar Nasional Teknologi Informasi & Komunikasi Terapan 2011 (Semantik 2011)*, 2011, pp. 1–6.

[20] M. A. I. Pakereng, Y. R. Beeh, and S. Endrawan, "Perbandingan Steganografi Metode Spread Spectrum dan Least Significant Bit (LSB) antara Waktu Proses dan Ukuran File Gambar," *J. Inform.*, vol. 6, no. 1, pp. 68–86, 2010.

[21] Z. Niswati, "Steganografi berbasis Least Significant Bit (LSB) untuk Menyisipkan Gambar ke dalam Citra Gambar," *Fakt. Exacta*, vol. 5, no. 2, pp. 181–191, 2007.

[22] Adiria, "Analisis dan perancangan aplikasi steganografi pada citra digital menggunakan metode LSB) (Least Significant Bit)," UIN Syarif Hidayatullah Jakarta, 2010.

[23] S. Gupta, A. Goyal, and B. Bhushan, "Information Hiding using Least Significant Bit Steganography and Cryptography," *I.J.Modern Educ. Comput. Sci.*, vol. 6, no. 6, pp. 27–34, 2012.

[24] L. M. Marvel, C. G. Boncelet, and C. T. Retter, "Methodology of Spread-Spectrum Image Steganography," *ARMY Res. Lab.*, pp. 1–25, 1998.

[25] P.-Y. Chen and H.-J. Lin, "A DWT Based Approach for Image Steganography," *Int. J. Appl. Sci. Eng.*, vol. 4, no. 3, pp. 275–290, 2006.

[26] M. K. Ramani, E. V. Prasad, and S. Varadarajan, "Steganography using BPCS to the Integer Wavelet Transformed Image," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 7, no. 7, pp. 293–302, 2007.

[27] A. Prawirawan, I. Isnawaty, and R. Ramadhan, "Implementasi Discrete Wavelet Transform untuk Penyisipan Teks pada Gambar," *semanTIK*, vol. 1, no. 1, pp. 11–18, 2015.